

REMARKS/ARGUMENTS

Claims 1-70 stand rejected based on the U.S. Patent Publication No. 2002/0174335 to Zhang et al (*hereinafter* Zhang). Claims 1-70 have been cancelled. For reasons that will now be set forth, new claims 71-100 are not anticipated by Zhang.

Independent claim 71 is directed to a system comprising an authentication server disposed on a network, a switch coupled to the network and communicatively coupled to the authentication server via the network and an access point communicatively coupled to the switch. The access point is configured to authenticate with the authentication server and establish a secure communication session with the switch. The access point is also configured to send a message to the switch comprising data representative of an authenticated wireless client responsive to the authenticated wireless client successfully authenticating with the authentication server. The access point forwards all communications received from the authenticated wireless client to the switch responsive to the authenticated wireless client successfully authenticating with the authentication server.

Similarly, independent claim 82 recites a system comprising an authentication server disposed on a network, a first authenticator communicatively coupled to the authentication server via the network and a first supplicant communicatively coupled to the first authenticator. The first supplicant is configured to authenticate with the authentication server and establish a secure communication session with the first authenticator. The first supplicant is also configured to function as an authenticator for a second supplicant communicatively coupled to the first supplicant. The first supplicant is further configured to send a message with data representative of the second supplicant to the first authenticator responsive to the second supplicant successfully authenticating with the authentication server and to forward all communications received from the second supplicant to the first authenticator responsive to the second supplicant successfully authenticating with the authentication server. Independent claim 90 recites a method for implementing the functionality of a supplicant that subsequently functions as an authenticator (e.g. the second supplicant recited in claim 82 or an access point as recited in claim 71) and independent claim 94 recites a method for implementing the functionality of an authenticator (e.g. the first authenticator recited in claim 82 or the switch recited in claim 71).

By contrast, Zhang teaches that “the AP 120 and each authentication server 150 share a secret and all RADIUS packets exchanged between them are authenticated using this secret together with a random authenticator:” (Zhang, para. 72). Upon a successful authentication, he access point forwards the user SS2 (a message encrypted with the user’s password), the user’s session key and a WEP broadcast key to the mobile terminal (para. 82). However, nowhere does Zhang disclose that a secure communication session is established between the AP/first supplicant (e.g. Wireless LAN Access Point 120 in Zhang) and the switch/first authenticator (e.g. Internet Interface 130 in Zhang). Furthermore, nowhere does Zhang disclose that upon successful authentication of the wireless client (e.g. M.T. 120 in Zhang) that the AP/second supplicant (e.g. AP 120 in Zhang) sends a message containing data representative of the wireless client/second supplicant (e.g. MT 120 in Zhang) to the switch/first authenticator (e.g. the Internet Interface 130 in Zhang). All Zhang teaches is that upon a successful authentication, the AP forwards all packets from MT 120 unfiltered. Therefore, Zhang does not disclose each and every element of independent claims 71, 82, 90 and 94.

Claims 72-81 directly depend from claim 71 and thus contain each and every element of claim 71. Therefore, for the reasons already set forth for claim 71, claims 72-81 are also not anticipated by Zhang. Claims 82-89 directly depend from claim 81 and thus contain each and every element of claim 81. Therefore, for the reasons already set forth for claim 81, claims 82-89 are also not anticipated by Zhang. Claims 91-93 directly depend from claim 90 and thus contain each and every element of claim 90. Therefore, for the reasons already set forth for claim 90, claims 91-97 are also not anticipated by Zhang. Claims 95-109 directly depend from claim 94 and thus contain each and every element of claim 94. Therefore, for the reasons already set forth for claim 94, claims 95-100 are also not anticipated by Zhang.

In addition to the reasons just set forth above, claim 72 recites that switch maintains a table of authorized users and updates the table with the medium access control (MAC) addresses of the authenticated wireless client. Claim 73 recites that the table also includes access control list (ACL) and Quality of Service (QoS) parameter for the authorized wireless client. Nothing in Zhang teaches that the Internet Interface 130 maintains such a table. Claims 83 and 84 recite similar elements to claims 72 and 73 respectively. Claims 95, 96 also recite similar elements to claims 72 and 73 respectively.

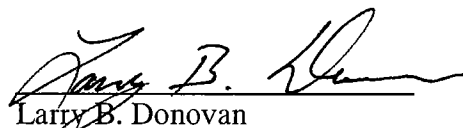
In addition to the reasons set forth above, claim 76 recites that a message authentication check key is used to identify the access point to the switch and claim 77 recites that the message authentication check key is used to verify the data representative of the authorized wireless client was sent by the access key. Zhang only teaches that an authenticated session is between the AP and the Authentication Server (para. 120), not between the AP and the switch (e.g. AP 120 and Internet Interface 130). Claims 86 and 87 contain similar elements to claims 76 and 77 respectively. Claims 94 and 95 contain similar elements to claims 76 and 77 respectively.

In addition to the reasons set forth above, claim 79 recites that the switch stores the MAC address for the authenticated wireless client in a database and the switch is responsive to receiving packets from the authenticated wireless client forwarded by the access point to verify the MAC address of the authenticated wireless client (moreover, claim 79 depends from claim 78 which recites that the switch also verifies the MAC address of the AP sending the data representative of the authenticated wireless client). Nothing in Zhang teaches this. In Zhang, the switch (internet interface 130) merely forwards any packets forwarded to it by AP 120, the switch (internet interface) in Zhang does not verify the MAC address of the mobile terminal before forwarding the packets. Claim 100 also recites similar elements to claim 79.

Therefore, for the reasons set forth above, the claims as currently standing are not anticipated by Zhang. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/08267.

Respectfully submitted,

Date: December 28, 2006



Larry B. Donovan
Registration No. 47,230
TUCKER ELLIS & WEST LLP
1150 Huntington Bldg.
925 Euclid Ave.
Cleveland, Ohio 44115-1414
Customer No.: 23380
Tel.: (216) 696-3864
Fax: (216) 592-5009